

IN THE CLAIMS:

1. (Currently amended) A computer-implemented method in a data processing system for reporting security situations, comprising the computer-implemented steps of:
in a first correlation server in a hierarchy of correlation servers, logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;
calculating a respective severity level levels for each of the groups;
calculating a delta severities severity for each group from the respective severity level and a respective prior severity level levels; and
for each group having a non-zero delta severity, propagating the respective delta severities severity to a higher-level correlation server.
2. (Currently amended) The computer-implemented method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.
3. (Currently amended) The computer-implemented method of claim 1, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.
4. (Currently amended) The computer-implemented method of claim 1, further comprising:
calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

5. (Currently amended) The computer-implemented method of claim 1, wherein the target attribute represents one of a computer and a collection of computers.
6. (Currently amended) The computer-implemented method of claim 1, wherein the source attribute represents one of a computer and a collection of computers.
7. (Currently amended) The computer-implemented method of claim 1, further comprising: aggregating a subset of the groups into a combined group.
- 8-10. (Cancelled)
11. (Currently amended) A computer program product, ~~in a computer-readable medium for reporting security events, comprising instructions for:~~
a recordable-type media having computer-readable instructions including
first instructions, in a first correlation server in a hierarchy of correlation servers, for
logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
second instructions for classifying events as groups by aggregating events with at least
one attribute within the event set as an identical value;
third instructions for calculating a severity level levels for each of the groups;
fourth instructions for calculating a delta severities severity for each group from the
respective severity level and a prior severity level levels; and
fifth instructions for propagating, for each group having a non-zero delta severity, the
delta severities severity to a higher-level correlation server.
12. (Original) The computer program product of claim 11, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

13. (Original) The computer program product of claim 11, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

14. (Currently amended) The computer program product of claim 11, ~~comprising additional instructions for~~ wherein the computer-readable instructions further include:

sixth instructions for calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

15. (Original) The computer program product of claim 11, wherein the target attribute represents one of a computer and a collection of computers.

16. (Original) The computer program product of claim 11, wherein the source attribute represents one of a computer and a collection of computers.

17. (Currently amended) The computer program product of claim 11, ~~comprising additional instructions for~~ wherein the computer-readable instructions further include:

seventh instructions for aggregating a subset of the groups into a combined group.

18-20. (Cancelled)

21. (Currently amended) A data processing system for reporting security events, comprising:
a first bus system;
a first memory;
a first processing unit connected as a first correlation server in a hierarchy of correlation servers, wherein the first processing unit includes at least one processor; and
a first set of instructions within the first memory,
wherein the first processing unit executes the first set of instructions to perform the acts of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;
calculating a severity level levels for each of the groups;
calculating a delta severities severity for each group from the respective severity level and a prior severity level levels; and
for each group having a non-zero delta severity, propagating the delta severities severity to a higher-level correlation server.

22. (Original) The data processing system of claim 21, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

23. (Original) The data processing system of claim 21, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

24. (Original) The data processing system of claim 21, wherein the processing unit executes the set of instructions to perform the act of:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

25. (Original) The data processing system of claim 21, wherein the target attribute represents one of a computer and a collection of computers.

26. (Original) The data processing system of claim 21, wherein the source attribute represents one of a computer and a collection of computers.

27. (Original) The data processing system of claim 21, wherein the processing unit executes the set of instructions to perform the act of:

aggregating a subset of the groups into a combined group.

28-30. (Cancelled)

31. (New) The computer-implemented method of claim 1, further comprising:

receiving, in the higher-level correlation server, a plurality of delta packets from a plurality of lower-level correlation servers that include the first correlation server, wherein each delta packet contains the respective delta severity for each group of the respective lower-level correlation server that has a non-zero delta severity;

performing a first mathematical operation on the plurality of delta packets to form a new delta packet;

if the higher-level correlation server is the top level of the hierarchy of correlation servers, performing a second mathematical operation on the new delta packet and a stored severity packet to form a new severity packet; and

if the higher-level correlation server is not the top level of the hierarchy of correlation servers, propagating the new delta packet to a higher-level correlation server.

32. (New) The computer-implemented method of claim 31, wherein the first mathematical operation and the second mathematical operation are each one of addition, arithmetic mean, and geometric mean.

33. (New) The computer-implemented method of claim 31, further comprising presenting to an operator each group which has a respective severity value in the new severity packet that is greater than a respective threshold.

34. (New) The computer program product of claim 11, further comprising instructions for: receiving, in the higher-level correlation server, a plurality of delta packets from a plurality of lower-level correlation servers that include the first correlation server, wherein each

delta packet contains the respective delta severity for each group of the respective lower-level correlation server that has a non-zero delta severity;

performing a first mathematical operation on the plurality of delta packets to form a new delta packet;

if the data processing system is the top level of the hierarchy of servers, performing a second mathematical operation on the new delta packet and a stored severity packet to form a new severity packet; and

if the data processing system is not the top level of the hierarchy of servers, propagating the new delta packet to a higher-level correlation server.

35. (New) The computer program product of claim 34, wherein the first mathematical operation and the second mathematical operation are each one of addition, arithmetic mean, and geometric mean.

36. (New) The computer program product of claim 34, further comprising presenting to an operator each group that has a respective severity value in the new severity packet that is greater than a respective threshold.

37. (New) The data processing system of claim 21, further comprising:
a second bus system;
a second memory;
a second set of instructions within the second memory; and
a second processing unit connected as the higher-level correlation server;
wherein the second processing unit executes the second set of instructions to perform the acts of:

receiving, from the first correlation server and a third correlation server, a first delta packet and a second delta packet, wherein said first delta packet contains the respective delta severity for each group of the first correlation server that has a non-zero delta severity and the second delta packet contains a respective delta severity for each group of the third correlation server that has a non-zero delta severity;

performing a first mathematical operation on the first delta packet and the second delta packet to form a new delta packet;

if the data processing system is the top level of a hierarchy of servers, performing a second mathematical operation on the new delta packet and a stored severity packet to form a new severity packet; and

if the data processing system is not the top level of a hierarchy of servers, propagating the new delta packet to a higher-level correlation server.

38. (New) The computer program product of claim 37, wherein the first mathematical operation and the second mathematical operation are each one of addition, arithmetic mean, and geometric mean.

39. (New) The computer program product of claim 37, further comprising presenting to an operator each group which has a respective severity value in the new severity packet that is greater than a respective threshold.